ent services such as personal services or employer provided services. Accordingly, another set of credentials may be stored in the access server database and associated with a unique key (e.g., key B). When these other credentials are presented to the access device **304**, the key B will be provided to the access device **304** using the secure techniques discussed above. Accordingly, access device may use the key B **350** to establish a separate, cryptographically secure connection to a network.

[**0092**] These aspects of the invention will be described in more detail in conjunction with **FIGS. 5 and 6**. **FIG. 5** is a simplified diagram of one embodiment of a network system that may support a variety of communication and data processing devices.

[**0093**] In **FIG. 5** access devices connect to a wide area network ("WAN") **502** such as the Internet via an access point (e.g., a router) **504**. Here, the access point may serve as the access server discussed herein. Alternatively, the access point **504** may connect to an access server (not shown) such that the credentials and keys pass through the access point as they are sent between the access server and the access devices. In either case, credentials for any users that are authorized to access the system may be enrolled with the access server.

[**0094**] The access point **504** may provide connectivity for wired or wireless devices. For example, a network printer **512** may be connected to the access point by a wired connection as represented by line **506**. A voice-over-Internet-Protocol ("VoIP") phone **514** also may connect to the access point via a wired connection as represented by line **508**.

[**0095**] Other devices may connect to the access point via radio frequency ("RF") signals as represented, for example, by the curved lines **510**. Here, the access point **504** may support wireless standards such as Bluetooth, 802.11, GSM, etc.

[**0096**] Examples of access devices include a VoIP phone **514** that supports the Bluetooth protocol; a laptop computer **516** that supports 802.11 and/or Bluetooth; a personal digital assistant ("PDA") **518** that supports 802.11 and/or Bluetooth and may include a cellular telephone that supports, for example GSM; a personal entertainment device **520**; a phone **522** that supports GSM and/or 802.11 and that communicates with peripherals such as a wireless headset **524** via Bluetooth; and a personal computer **526** that supports an 802.11 wireless connection and that communicates with wireless peripherals such as a Bluetooth-enabled keyboard **528** and mouse **530**.

[**0097**] As discussed herein, each of the devices **512-530** may include a security module (not shown) that enables the device to securely and efficiently receive any keys necessary to connect to the data network **502** and/or to other devices. In the latter case, for example, keys may be securely distributed between devices to enable a peripheral (e.g., keyboard **528**) to securely communicate with a base device (e.g., computer **526**). Accordingly, users may connect any of these devices to the network or other devices by simply providing their credentials to one or more input devices **536** which then route the credentials to the device(s) as discussed herein. For example, an input device **536** may communicate with a device **512-530** to provide a credential to a device **512-530**. In the case of the peripherals (e.g., keyboard **528**), the credentials may be passed through the base device (e.g., computer **526**), then routed to the access server **504**.

[**0098**] Additional details of the authentication components and processes that may be incorporated into these devices are described herein. For example, several embodiments for providing credentials to an access device or an access server are discussed below in conjunction with **FIGS. 7-10**. In addition, several embodiments of security modules are discussed below in conjunction with **FIGS. 11-14**.

[**0099**] Referring to **FIG. 6**, a simplified flowchart is illustrated relating to operations that may be performed in a network system (e.g., as shown in **FIG. 5**). For example, such a system may include multiple access devices and support multiple users and multiple levels of credentials. In general, these operations may be performed as discussed herein, for example, in conjunction with **FIGS. 3 and 4**. For convenience, not all of the operations involved in the process are illustrated in **FIG. 6** or discussed below.

[**0100**] As represented by block **602**, a credential for a user (referred to for convenience as "user A") is enrolled with the access server. At block **604**, user A presents his or her credential to an input device that then sends the credential to an access device (referred to for convenience as "access device **1**"). The access device **1** sends the credential to the access server and, after the access server verifies that the credential has been enrolled, the access server sends the associated key(s) to the access device **1** (block **606**). Access device **1** may then use the key(s) associated with user A to connect to the network (block **608**).

[**0101**] Blocks **610-614** illustrate that a network may be automatically built as a user provides his or her credentials to multiple access devices in the system. As represented by block **610**, user A may provide his or her credential to another access device (referred to for convenience as "access device **2**") via the input device. The access device **2** sends the credential to the access server and, after the access server verifies that the credential has been enrolled, the access server sends the associated key(s) to the access device **2** (block **612**). Access device **2** may then use the key(s) associated with user A to connect to the network (block **614**).

[**0102**] Blocks **616-622** illustrate that a given device may be used by several users to access the network. Here, each of the users may be assigned different credentials. As represented by block **616**, a credential for another user (referred to for convenience as "user B") may be enrolled with the access server. At block **618**, user B also may provide his or her credential to the access device **1** via the input device. The access device **1** sends the credential to the access server and, after the access server verifies that the credential has been enrolled, the access server sends the associated key(s) to the access device **1** (block **620**). Access device **1** may then use the key(s) associated with user B to establish an entirely separate and cryptographically secure connection with the network (block **622**).

[**0103**] In practice, the separate set of credentials identified above as being associated with user B may be a second set of credentials assigned to a given user (e.g., user A). For example, a user may have one set of credentials assigned for one network (e.g., a home network) and another set of